



Miercom



Palo Alto Networks



Next Generation Firewall (NGFW)
Competitive Performance for
Distributed Enterprise and SMB Use Cases

Detailed Report DR210617G
Performance Validation Testing

MIERCOM.COM

CONTENTS

01 KEY FINDINGS	3
02 TEST SUMMARY	5
03 PRODUCTS TESTED	6
04 HOW WE DID IT	7
05 COMPARATIVE PERFORMANCE RESULTS	8
06 TOTAL COST OF OWNERSHIP	18
ABOUT MIERCOM	21
APPENDIX	22

KEY FINDINGS

1

Business networks are a hybrid of local, remote and mobile networks that each introduce their own range of threats and vulnerabilities. Administrators need to ensure the organization, and all of its users, can safely access critical resources without affecting productivity, speed or security.

By engaging Miercom to perform independent validation testing, Palo Alto Networks aimed to prove how deploying its security services on the firewalls can boost protection without degrading performance. The PA-410, PA-440, PA-450, and PA-460 NGFW appliances were compared to the Fortinet FortiGate (FG) FG-61F, FG-81F, FG-101F, and FG-201F for performance scenarios that customers can expect to experience in their networks.

Tests were run twice, once with all available services disabled (“services off”) and again with all services enabled (“services on”). Real-world deployments need services enabled for optimal protection. However, customers often turn services off in order to get acceptable performance - significantly compromising security. For Palo Alto Networks, “services on” involved turning on these features and services: Threat Prevention (AV, Vulnerability Protection, Anti-spyware, Data Filtering, File Blocking), Advanced URL Filtering, DNS Security, and WildFire. For Fortinet devices, “services on” involved turning on these features and services: Antivirus, Web Filter, IPS, File Filter, and Email Filter.

The Ixia BreakingPoint PerfectStorm test tool was used to push the limits of each competing platform, utilizing an 8x10-GE line card, for different scenarios commonly seen in Small Business (SMB) and Distributed Enterprise environments. Below are our findings.

Key Findings

- **Superior Throughput with Security Services Enabled.** Palo Alto Networks saw up to 6x higher throughput across all parameters tested, including application traffic.
- **Superior Real-world Application Traffic Performance.** On single application tests (MySQL, SIP and FIX), the Palo Alto Networks PA-400 Series performance shows consistently low degradation when services are enabled, with an average of 8%.
- **High Value, Low Cost of Ownership.** Palo Alto Networks showed higher performance and lower cost for every appliance compared to similar Fortinet products, with cost per Mbps up to 9x lower.

It is important to note that appropriate product size is considered when deploying a NGFW appliance. Metrics for each product were observed in the intended network environment to yield the optimal, but realistic, performance. We find datasheet claims do not show results of real-world deployments, or sometimes even with security services turned on, thus giving a false impression of protection and performance capabilities. Miercom used each product as any customer would, providing objective and practical results.

Based on our observations, we found the Palo Alto Networks Next Generation Firewall PA-410/440/450/460 appliances to have superior performance in multiple real-world network scenarios, with and without security features enabled. This series offered superior performance to its competitor, at a lower cost, making it a valuable investment for any network looking to boost security without sacrificing productivity and overhead expenses. We proudly award Palo Alto Networks the **Miercom Performance Verified** certification in recognition of its impressive competitive performance.

Rob Smithers

CEO, Miercom





Test Summary

	PA-410	FG-61F	PA-440	FG-81F	PA-450	FG-101F	PA-460	FG-201F
Average Throughput with Services Enabled (Mbps)	389.57	73.57	730.5	217.57	926.43	140.71	1,239.86	701.77
TCO per Protected Mbps (Pro-Bundle for Palo Alto Networks, UTP Bundle for Fortinet)	\$5.22	\$35.88	\$4.09	\$24.22	\$8.88	\$83.65	\$10.02	\$20.60
Throughput Comparison	PA-410 throughput is 5.3X better than FG-61F		PA-440 throughput is 3.4X better than FG-81F		PA-450 throughput is 6.6X better than FG-101F		PA-460 throughput is 1.8X better than FG-201F	
TCO Comparison	PA-410 TCO is 6.9X better than FG-61F		PA-440 TCO is 5.9X better than FG-81F		PA-450 TCO is 9.4X better than FG-101F		PA-460 TCO is 2.1X better than FG-201F	



Products Tested

Palo Alto Networks PA-410/440/450/460 Next Generation Firewall

These new additions to Palo Alto Networks' NGFW portfolio allow customers to deploy devices for enterprise branch, retail, commercial locations, and managed services deployments. Testing for the following products focused on small business (SMB) and branch/distributed enterprise use cases.



PA-410
Version 10.1.2-cl5



PA-440
Version 10.1.0-b23



PA-450
Version 10.1.0-b23



PA-460
Version 10.1.0-b23

Services on:

- Threat Prevention (AV, Vulnerability Protection, Anti-spyware, Data Filtering, File Blocking)
- Advanced URL Filtering
- DNS Security
- WildFire

Fortinet FortiGate FG-61F/81F/101F/201F Network Firewall



FG-61F
Version 7.0.0build0066(GA)



FG-81F
Version 6.4.5 build5656

Services on:

- Antivirus
- Web Filter
- IPS
- File Filter
- Email Filter



FG-101F
Version 7.0.0 build0066



FG-201F
Version 6.4.5 build5656

4

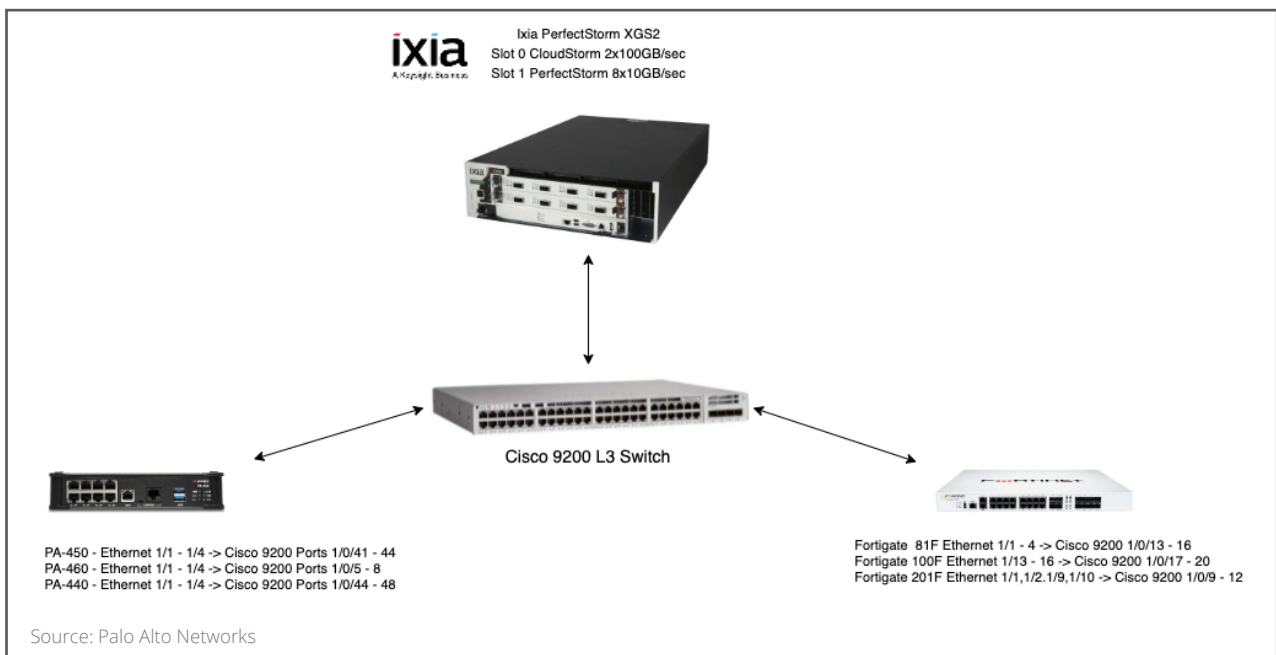
How We Did It

Using hands-on network testing tools, business environments were simulated and challenged with real-world traffic scenarios to provide an accurate assessment of product performance.

The Palo Alto Networks and Fortinet appliances were competitively compared using application traffic generated by Ixia PerfectStorm XGS2 (v9.10.110.25) while services were disabled/enabled on the device.

All devices were configured to have security disabled (“services off”) and then security enabled (“services on”). For Palo Alto Networks, “services on” involved turning on these features and services: Threat Prevention (AV, Vulnerability Protection, Anti-spyware, Data Filtering, File Blocking), Advanced URL Filtering, DNS Security, and WildFire. For Fortinet devices, “services on” involved turning on these features and services: Antivirus, Web Filter, IPS, File Filter, and Email Filter.

Test Topology

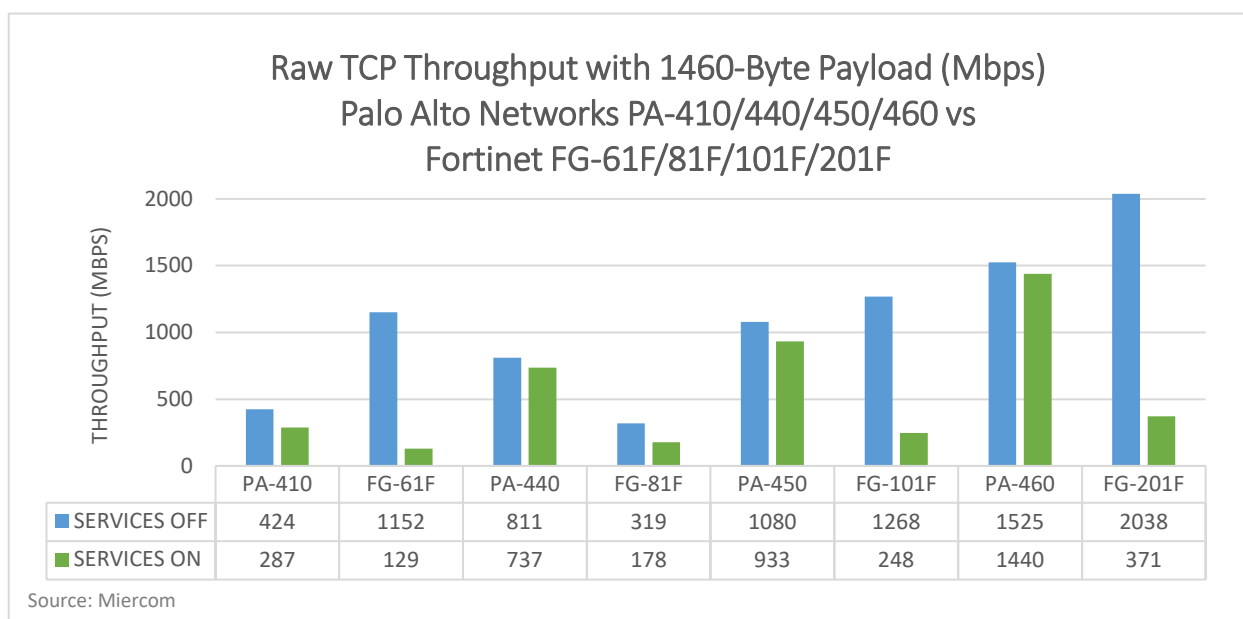


The Palo Alto PA-410/440/450/460 and Fortinet FG-61F/81F/101F/201F were the Device Under Tests (DUTs) connected to the client and server sides of the Ixia PerfectStorm XGS2 8x10-GE line card for traffic generation, testing, reporting, and packet captures. Tests began with 1,000 sessions, incrementing by 1,000 sessions every 10 seconds.

Comparative Performance Results



5.1 Raw TCP Throughput with 1460-Byte Payload



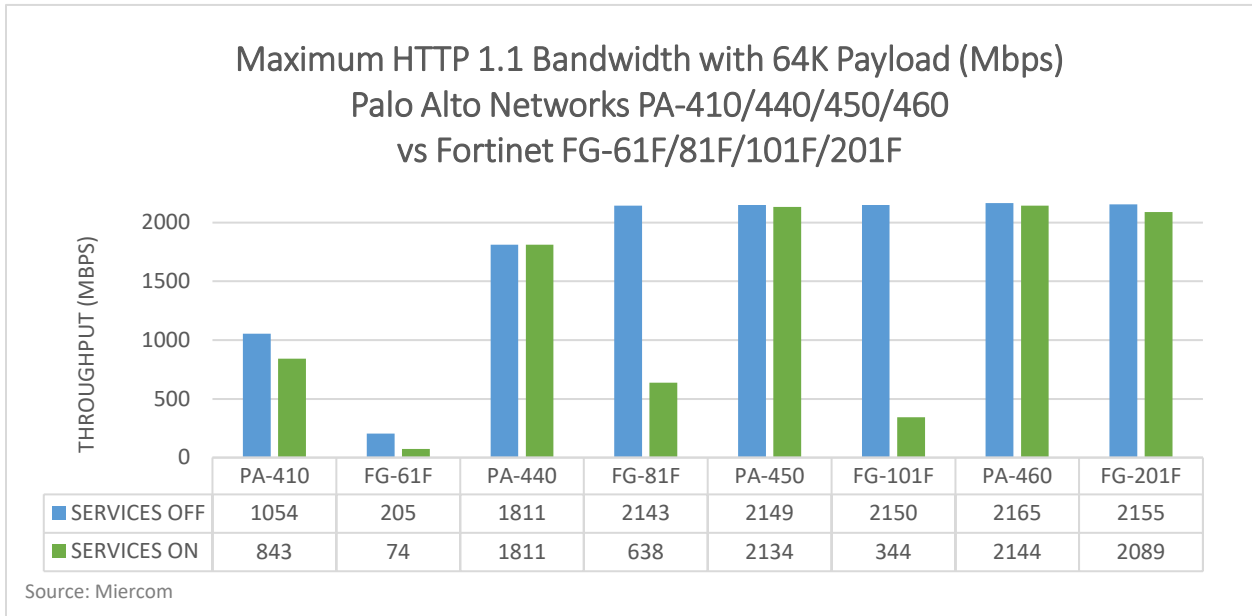
Palo Alto Networks PA-410 degraded by just 32 percent, while Fortinet FG-61F fell by 89 percent once services were enabled. PA-440 saw a 9.1 percent degradation with services enabled, but Fortinet FG-81F performance dropped by over 44 percent. PA-450 degraded by 13.6 percent compared to Fortinet FG-101F performance falling by more than 80 percent. PA-460 performance dropped 5.6 percent, with Fortinet FG-201F dropping by 82 percent.

The Palo Alto Networks Advantage

For all Palo Alto Networks appliances, Palo Alto Networks saw an average of just 15 percent degradation in performance with services enabled, faring much better than Fortinet which had an average of 74 percent reduced performance.

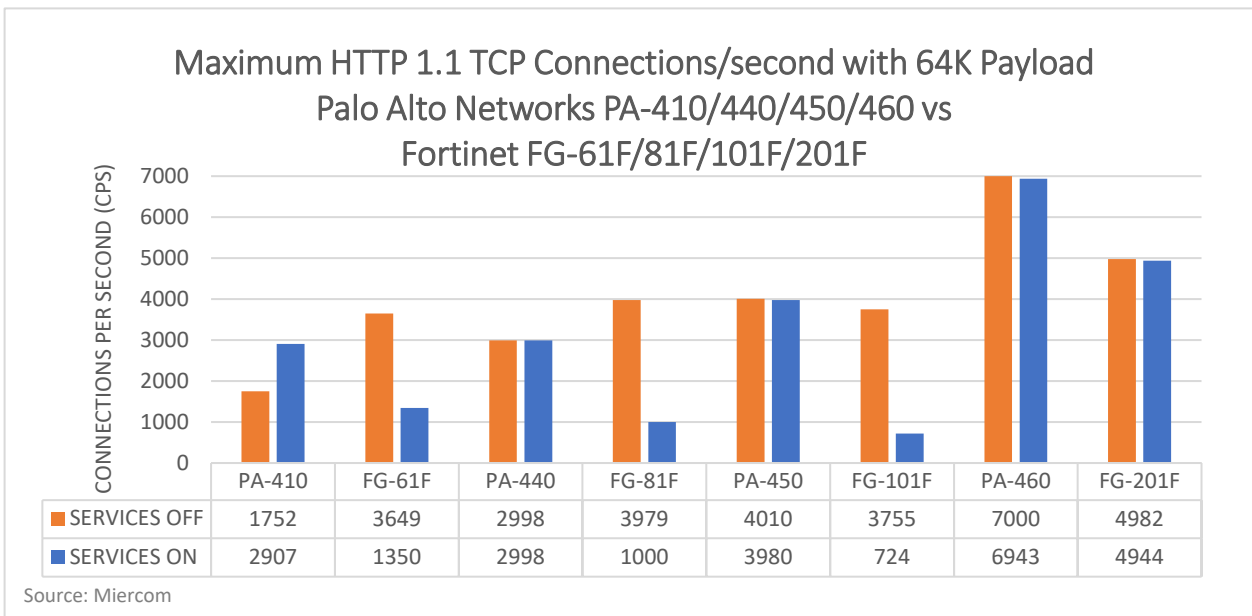
5.2 Maximum HTTP 1.1 Bandwidth & Connections/sec (CPS)

5.2.1 Bandwidth with 64K Payload (Mbps)



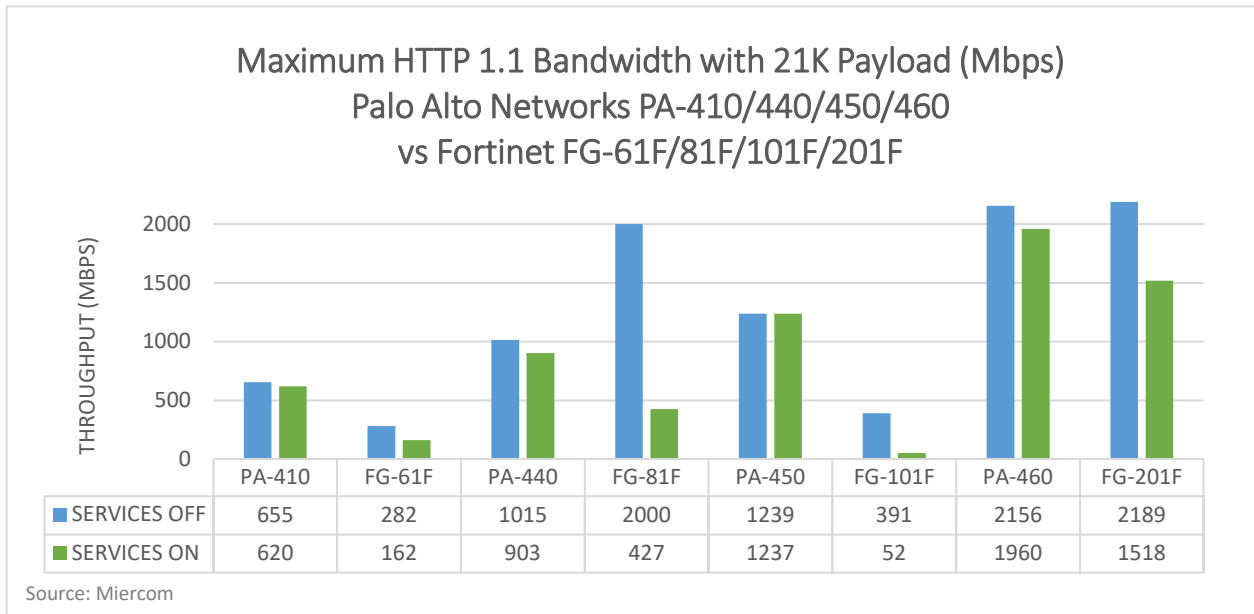
For a 64K payload, Palo Alto Networks PA-410 degraded by 20 percent with services enabled, while Fortinet FG-61F performance fell by 64 percent. PA-440 saw no degradation; FG-81F performance dropped by over 70 percent. PA-450 saw negligible degradation of 0.7 percent, while FG-101F dropped by 84 percent. Both PA-460 and FG-201F saw little degradation; PA-460 fell by 0.97 percent and FG-201F by 3 percent.

5.2.2 Connections/sec (CPS) with 64K Payload (Mbps)



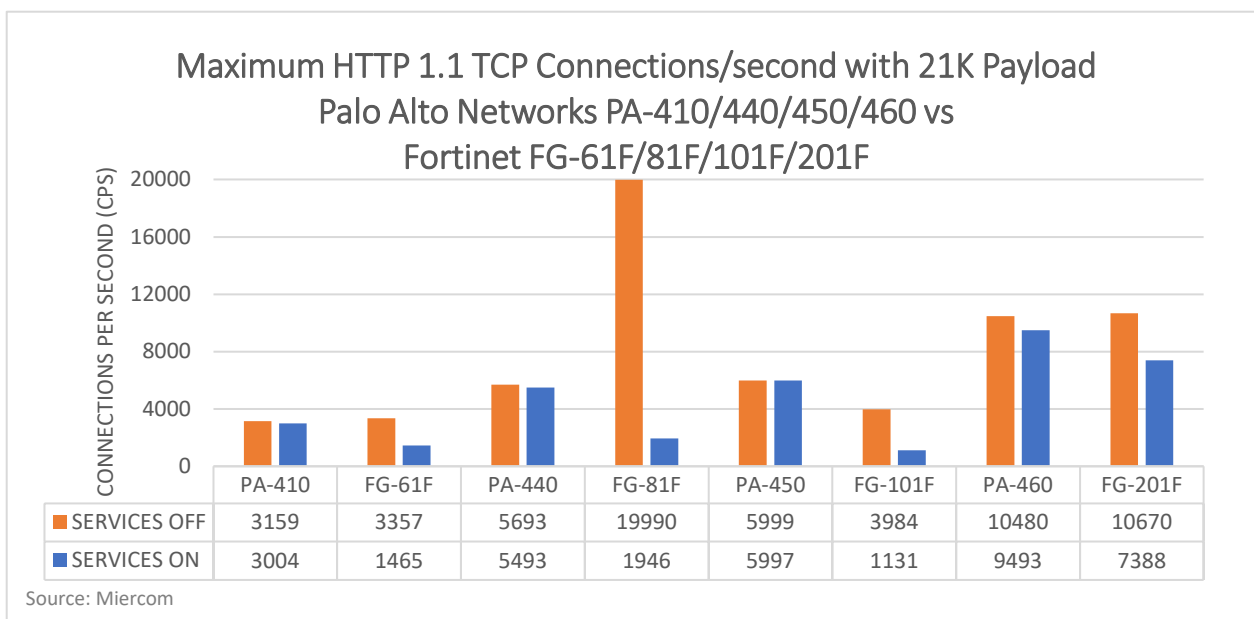
For a 64K payload, Palo Alto Networks PA-410 connection rate improved by 66 percent once services were enabled, with Fortinet FG-61F degrading by 63 percent. PA-440 saw no change in connection rate, while FG-81F dropped by 75 percent. PA-450 degraded by a 0.75 percent, with Fortinet FG-101F dropping by 81 percent. Both PA-460 and FG-201F connection rates had insignificant change with services enabled - a 0.8 percent drop for both appliances

5.2.3 Bandwidth with 21K Payload (Mbps)



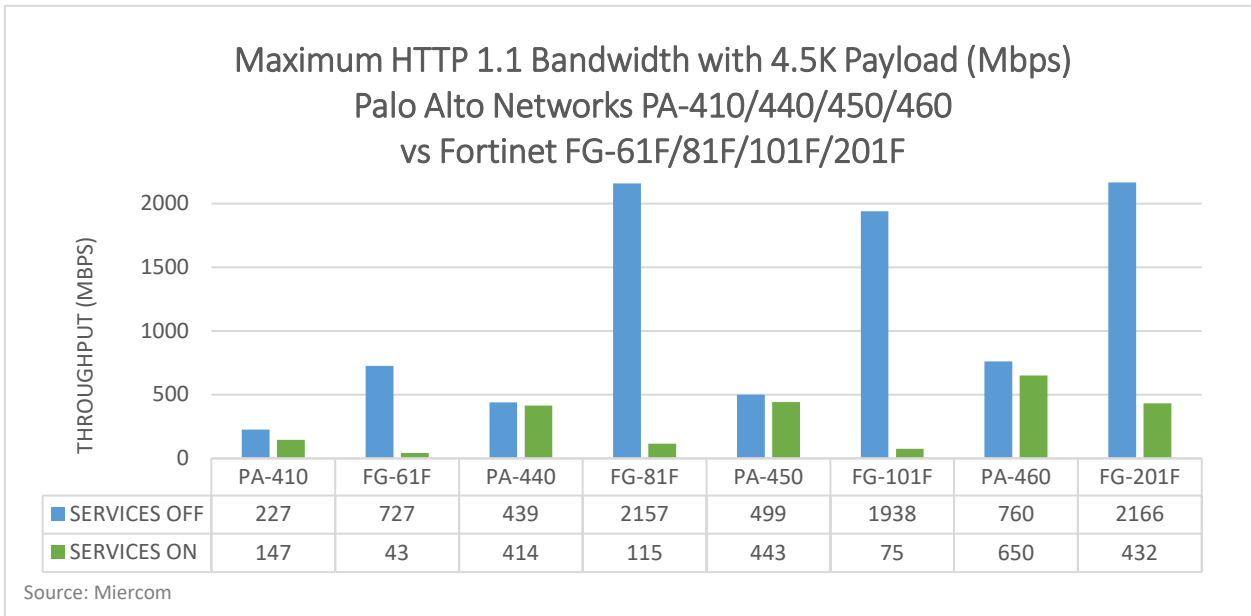
For 21K payload, Palo Alto Networks PA-410 bandwidth declined by a low 5 percent once services were enabled, with Fortinet FG-61F having a loss of 43 percent. PA-440 degraded by 11 percent, compared to the 79 percent loss seen by FG-81F. PA-450 barely fell at 0.2 percent, while FG-101F bandwidth decreased by 87 percent. PA-460 degraded by just 9 percent compared with FG-201F dropping by 31 percent once services were turned on.

5.2.4 Connections/sec (CPS) with 21K Payload (Mbps)



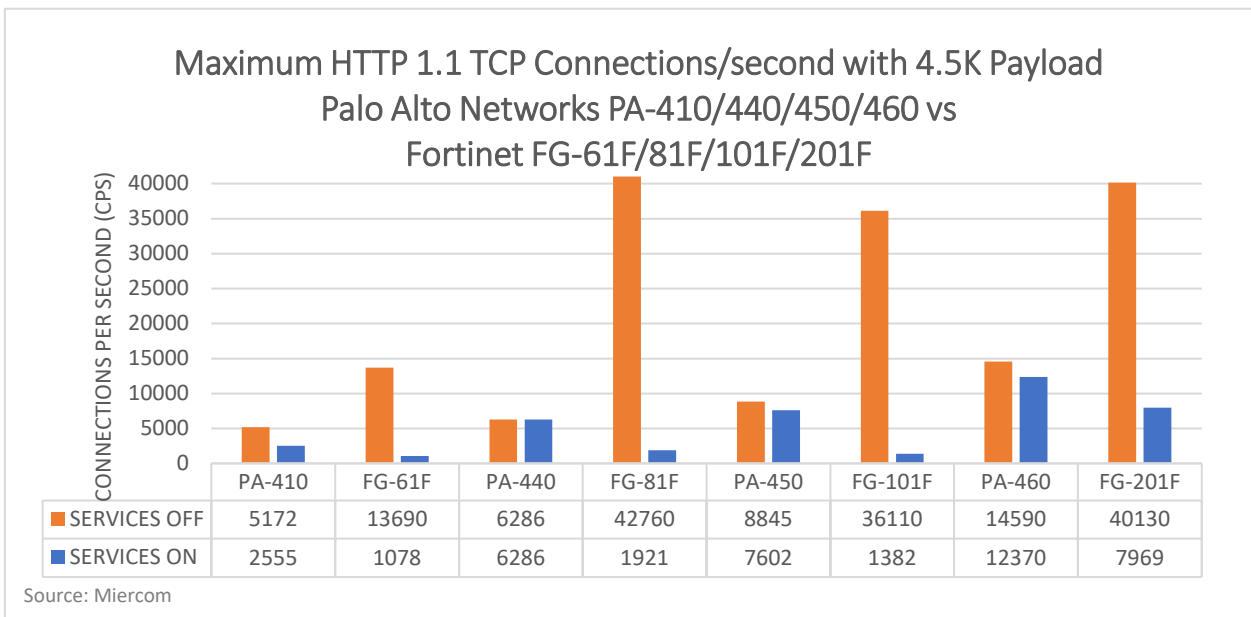
For 21K payload, Palo Alto Networks PA-410 connection rate saw little degradation of just 5 percent once services were enabled, compared to Fortinet FG-61F falling 56 percent. PA-440 connection rate dropped by just 3.5 percent, while Fortinet FG-81F fell by over 90 percent. PA-450 connection rate was essentially the same, falling by just 0.03 percent, unlike Fortinet FG-101F which fell by 72 percent. PA-460 connection rate degraded by just 9.4 percent and Fortinet FG-201F dropped by 31 percent once services were turned on.

5.2.5 Bandwidth with 4.5K Payload (Mbps)



For a 4.5K payload, Palo Alto Networks PA-410 bandwidth declined by 35 percent with services turned on, but Fortinet FG-61F saw a significant loss of over 94 percent. PA-440 saw just 5.7 percent degradation, whereas FG-81F dropped by 95 percent. PA-450 bandwidth degraded by just 11 percent, compared to FG-101F decreasing by over 96 percent. PA-460 degraded by just 14.5 percent, whereas FG-201F dropped by 80 percent once services were turned on.

5.2.6 Connections/sec (CPS) with 4.5K Payload (Mbps)



For a 4.5K payload, Palo Alto Networks PA-410 connection rate declined by 51 percent with services turned on, but Fortinet FG-61F saw significant loss of over 92 percent. PA-440 saw no change in connection rate when services were enabled, but FG-81F degraded by 96 percent. PA-450 connection rate degraded by 14 percent, compared with FG-101F dropping by more than 96 percent. PA-460 connection rate degraded by 15 percent and FG-201F dropped by 80 percent.

The Palo Alto Networks Advantage

Palo Alto Networks saw much less degradation than Fortinet once services were enabled - regardless of payload size. On average, Palo Alto Networks never saw degradation of more than 20 percent, with services enabled; Fortinet's degradation reached as high as 91 percent.

64K Payload

For bandwidth, Palo Alto Networks maintained sufficient performance when services were enabled - falling by just 5 percent on average. Fortinet had an average 55 percent loss in bandwidth. For connection rate, Palo Alto Networks had an average improvement of 16 percent. Fortinet appliances fell by an average of 55 percent.

21K Payload

For bandwidth, Palo Alto Networks maintained sufficient performance when services were enabled - falling by just 6 percent on average. Fortinet had an average 60 percent loss in bandwidth. For connection rate, Palo Alto Networks also saw little degradation - with an average of just 4.5 percent loss. Fortinet appliances fell by an average of 62 percent.

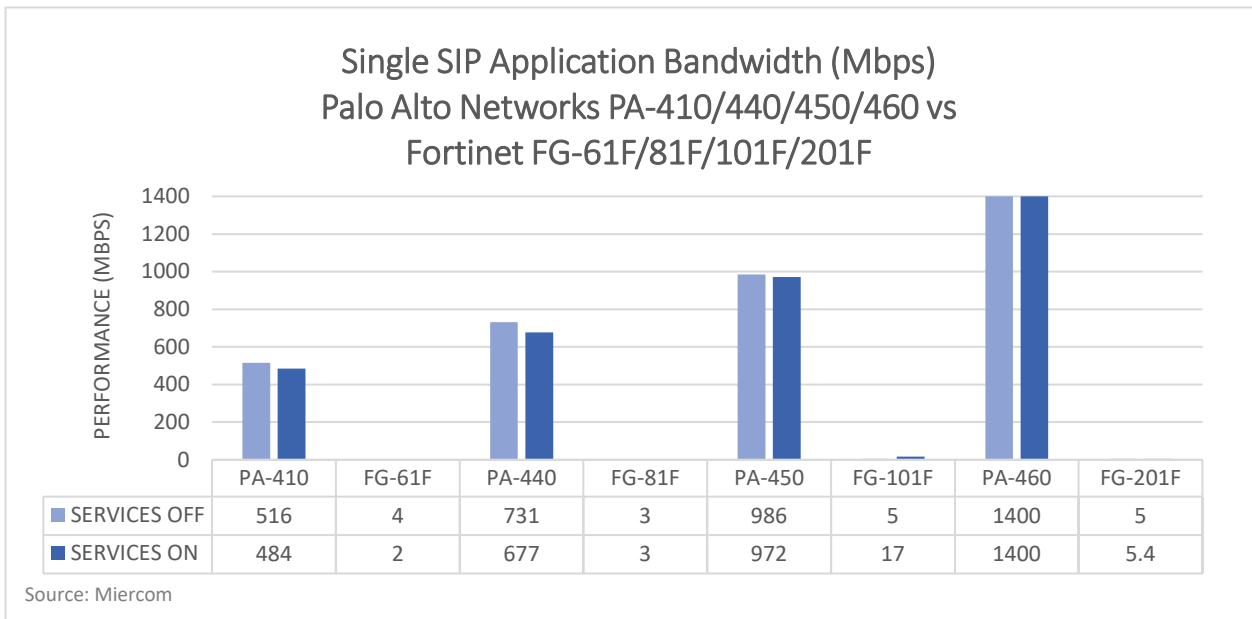
4.5K Payload

For bandwidth, Palo Alto Networks experienced a low average of 17 percent loss when services were enabled. Fortinet had a high loss in bandwidth - with an average of 91 percent degradation. For connection rate, Palo Alto Networks had an average of 20 percent decline in performance. Fortinet appliances, like bandwidth, saw a high loss of 91 percent on average.

5.3 Single Application Bandwidth

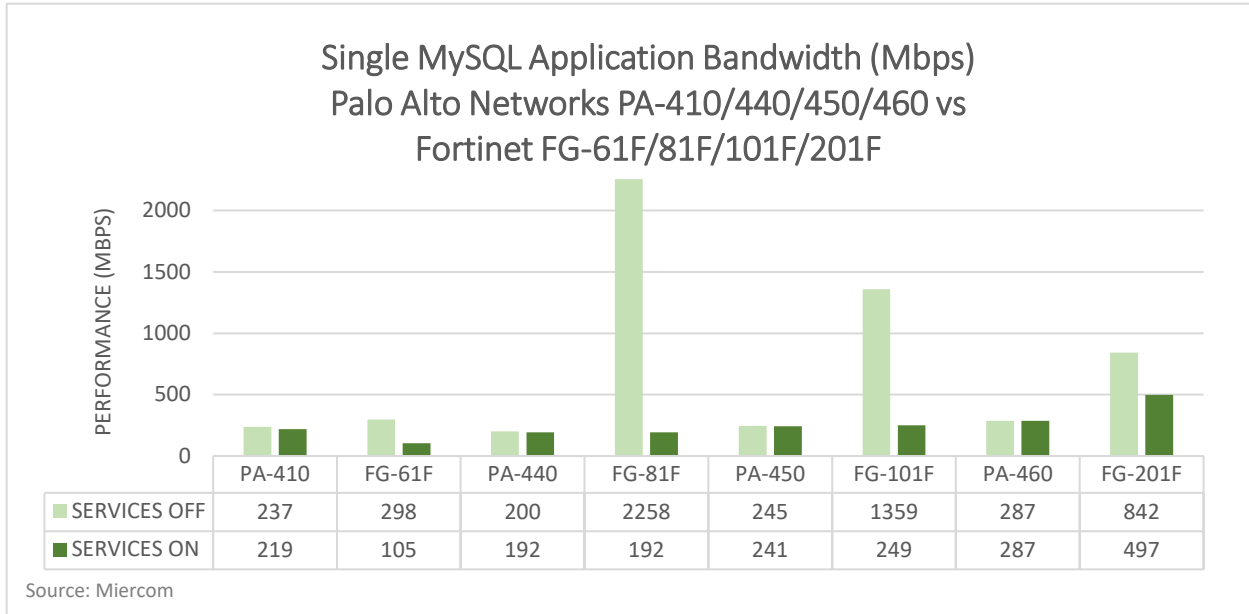
Fortinet devices showed very low SIP throughput. To work around the problem, the steps to disable SIP ALG listed in the knowledge base here (<https://kb.fortinet.com/kb/documentLink.do?externalID=FD36405>) were attempted, but it did not resolve the issue. It is our conclusion that SIP traffic is not being reliably processed by these Fortigate devices.

5.3.1 Session Initiation Protocol (SIP) Application Bandwidth



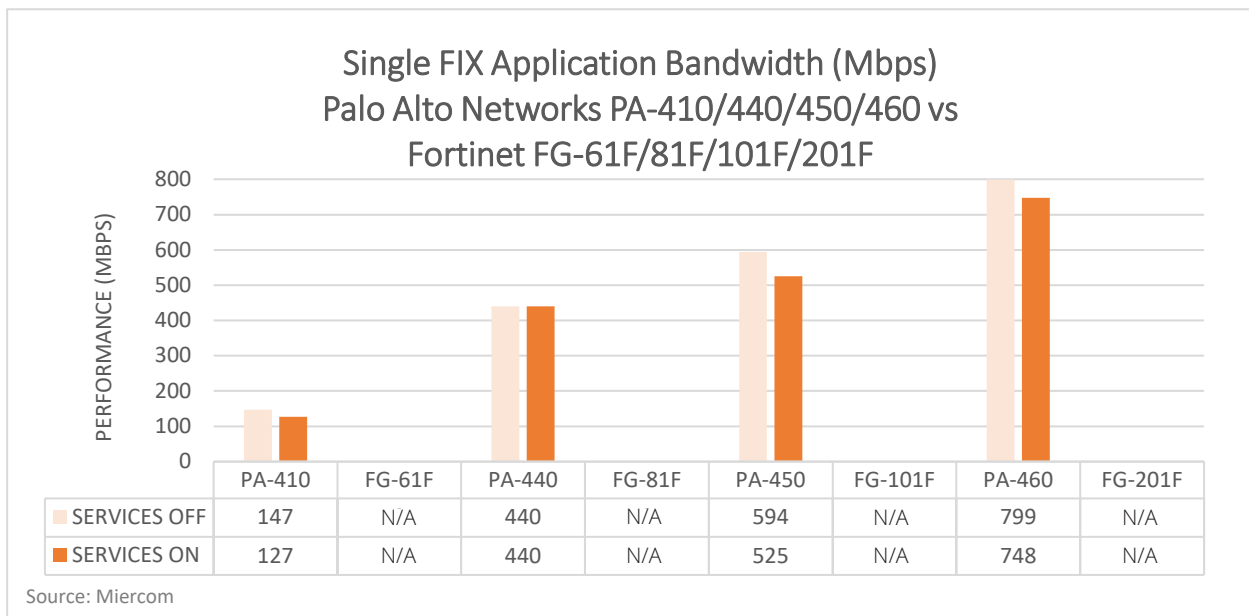
With services enabled, Palo Alto Networks PA-410 saw barely any loss in bandwidth at just 6 percent, compared to Fortinet FG-61F which degraded by 50 percent. While PA-440 had more degradation than FG-81F, by 7 percent, its throughput was 244 times that of Fortinet without services enabled and 226 times larger bandwidth when services were turned on. A similar situation was seen for PA-450, which degraded by 1 percent, compared to FG-101F improving by 240 percent. However, without services PA-450 had 197 times the throughput, and with services enabled, had 57 times the bandwidth. PA-460 bandwidth saw no loss with services enabled, compared to the improvement of 8 percent by FG-201F. Despite improvement from Fortinet, Palo Alto Networks showed 280 times the bandwidth without services enabled and 259 times the throughput when services were enabled.

5.3.2 MySQL Application Bandwidth



With services enabled, Palo Alto Networks PA-410 saw a 7.6 percent degradation, compared to Fortinet FG-61F having a 65 percent loss. PA-440 saw just 4 percent degradation, whereas FG-81F declined by 92 percent. PA-450 saw just 1.6 percent degradation; FG-101F declined by 82 percent. PA-460 saw no change once services were enabled, while FG-201F degraded by 41 percent.

5.3.3 Financial Information eXchange (FIX) Application Bandwidth



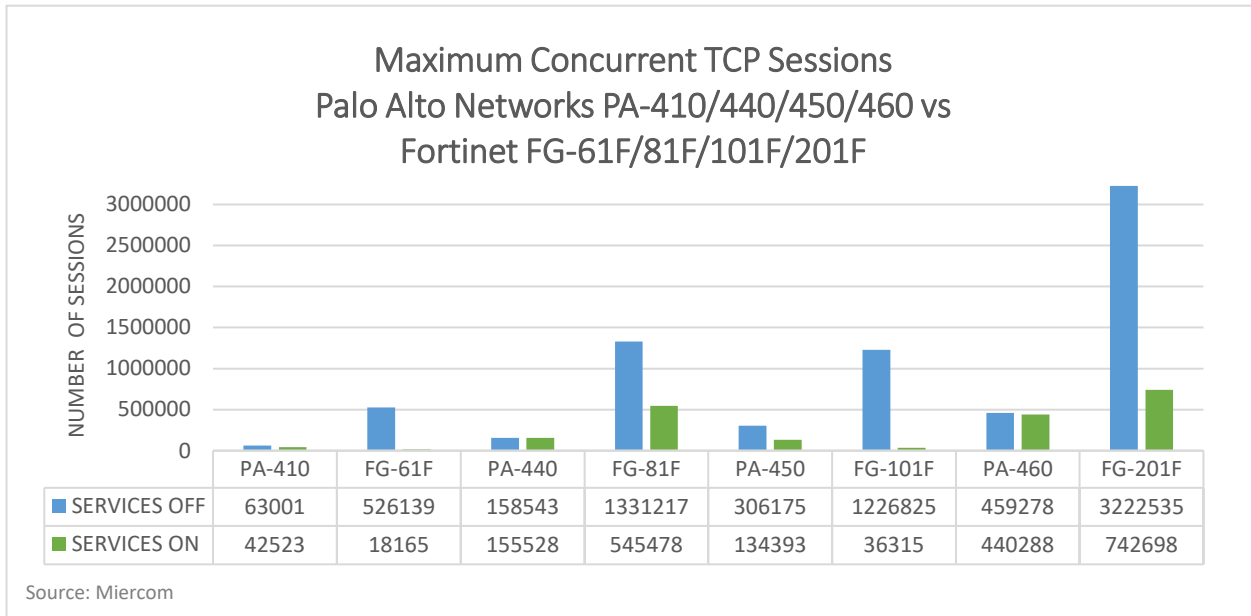
With services enabled, Palo Alto Networks PA-410 saw just 13.6 percent decline in performance. PA-440 saw no change in performance with services turned on. PA-450 had 11.6 percent degradation, and PA-460 had just 6 percent loss of bandwidth. No data was collected for Fortinet FG-61F/81F/101F/201F, as these appliances were unable to support FIX applications despite vendor recommendations to disable "FIX ALG".

The Palo Alto Networks Advantage

Fortigate platforms were unable to process FIX traffic causing 100 percent traffic loss. Fortigate platforms also achieved very low throughput for SIP protocol, making them not deployable where FIX or SIP protocols are required. The PA-400 series, on the other hand, was able to reliably process all three real-world applications tested with consistent performance even with services disabled.

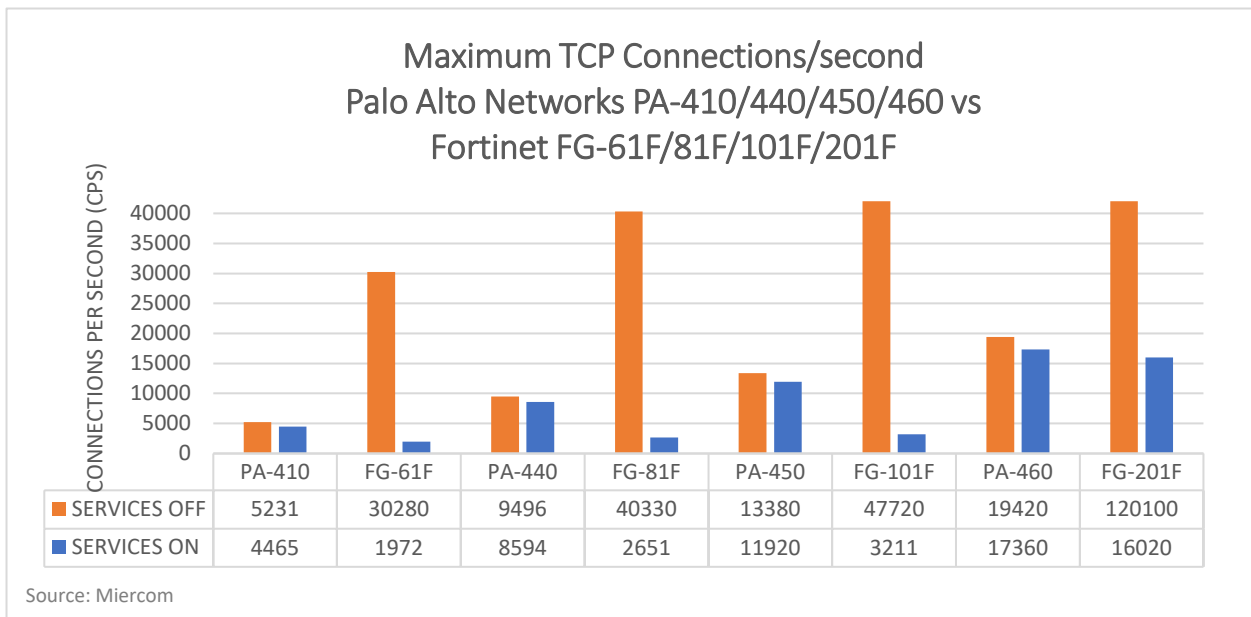
5.4 TCP Maximum Capacity

5.4.1 Maximum Concurrent TCP Sessions



Once services were enabled, Palo Alto Networks PA-410 session count degraded by 33 percent, compared to Fortinet FG-61F having a steep decline of 97 percent. PA-440 session count degraded by just 1.9 percent; FG-81F showed significantly more loss - of 59 percent. PA-450 degraded by 56 percent, compared to the severe degradation of 97 percent for FG-101F. PA-460 session count degraded by a 4 percent, while FG-201F saw degradation of 77 percent.

5.4.2 Maximum TCP Connections/sec (CPS)



Once services were enabled, Palo Alto Networks PA-410 connection rate declined by 15 percent; Fortinet FG-61F showed significant degradation of 94 percent. PA-440 fell by just 10 percent, while FG-81F dropped by over 93 percent. PA-450 experienced an 11 percent decrease, but FG-101F dropped by over 93 percent. PA-460 connection rate fell by 11 percent, compared to the 87 percent drop for FG-201F.

The Palo Alto Networks Advantage

Palo Alto Networks appliances were observed having an average 24 percent decline in TCP sessions once services were enabled. Fortinet had over 3 times the loss - at 82 percent average degradation. For connection rate, Palo Alto Networks experienced an average decline of just 11 percent, compared to Fortinet's significant 92 percent drop.

Total Cost of Ownership



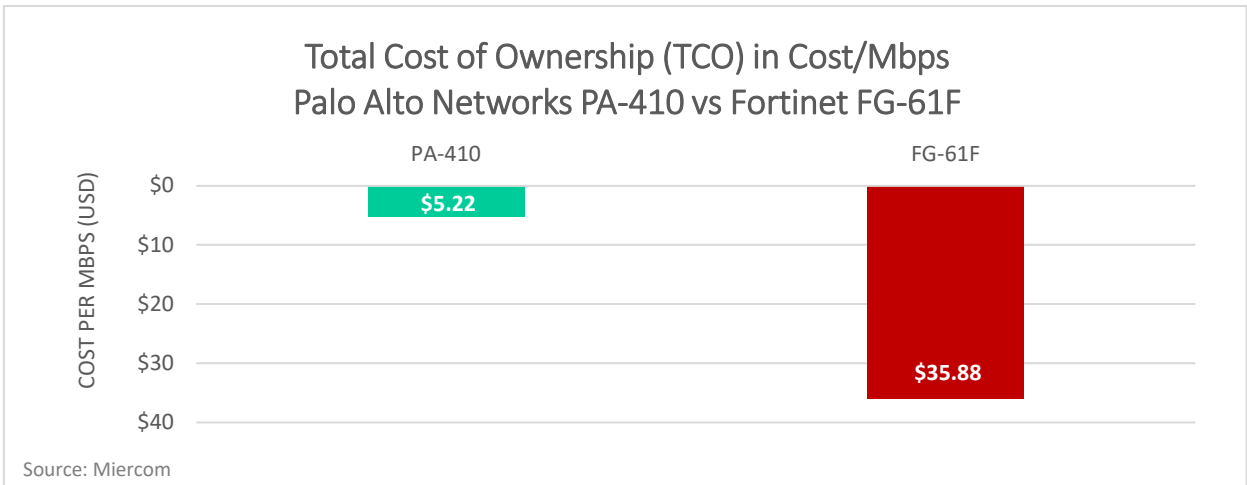
As with performance testing, we compared NGFW products for their performance and cost-benefit value in Cost per Mbps (USD). We evaluated the average throughput (in Mbps) and total cost of acquisition (hardware, subscription and support pricing). The following tables and charts provide details on the total Cost/Mbps calculations for each comparable pair.

Palo Alto Networks PA-400 Series TCO Calculations					
Product	Average Throughput (Mbps)	Total Cost (USD)	Hardware Cost (USD)	Subscription & Support Cost (USD)	Cost/Mbps
PA-410	389.57	\$2,035	\$695	\$1,340	\$5.22
PA-440	730.50	\$2,990	\$1,200	\$1,790	\$4.09
PA-450	926.43	\$8,230	\$2,800	\$5,430	\$8.88
PA-460	1,239.86	\$12,420	\$4,250	\$8,170	\$10.02

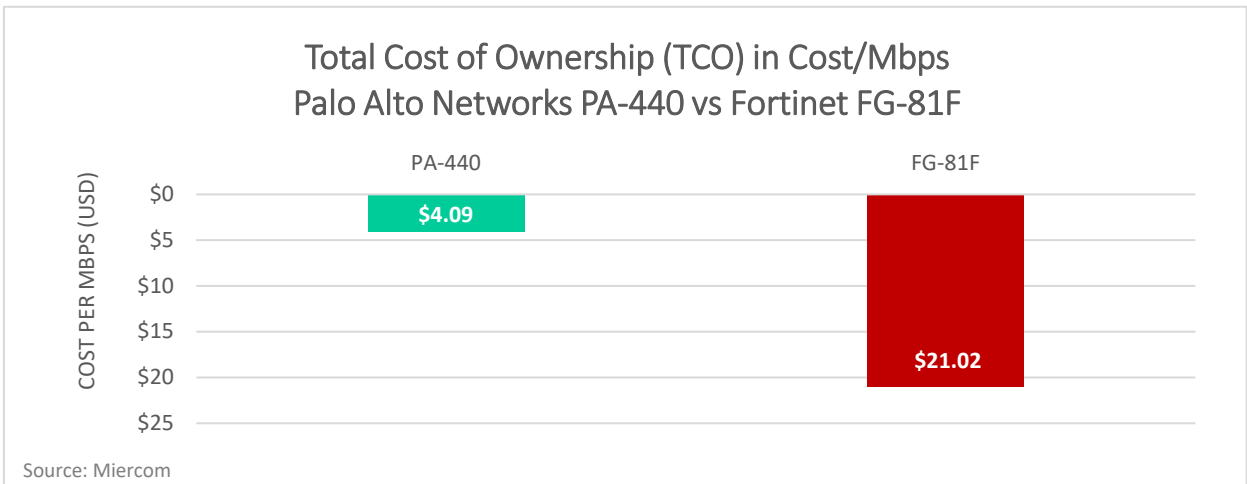
Fortinet FortiGate TCO Calculations					
Product	Average Throughput (Mbps)	Total Cost (USD)	Hardware Cost (USD)	Subscription & Support Cost (USD)	Cost/Mbps
FG-61F	73.57	\$2,640	\$895	\$1,745	\$35.88
FG-81F	217.57	\$4,573	\$1,550	\$3,023	\$21.02
FG-101F	140.71	\$11,771	\$3,990	\$7,781	\$83.65
FG-201F	701.77	\$14,455	\$4,900	\$9,555	\$20.60

Comparative Price and TCO Calculations: Palo Alto Networks vs Fortinet		
Product Comparison	Price Difference (Hardware and Subscriptions)	TCO per Protected Mbps Difference
PA-410 vs FG-61F	-22.9%	-85.5%
PA-440 vs FG-81F	-34.6%	-80.5%
PA-450 vs FG-101F	-30.1%	-89.4%
PA-460 vs FG-201F	-14.1%	-51.4%

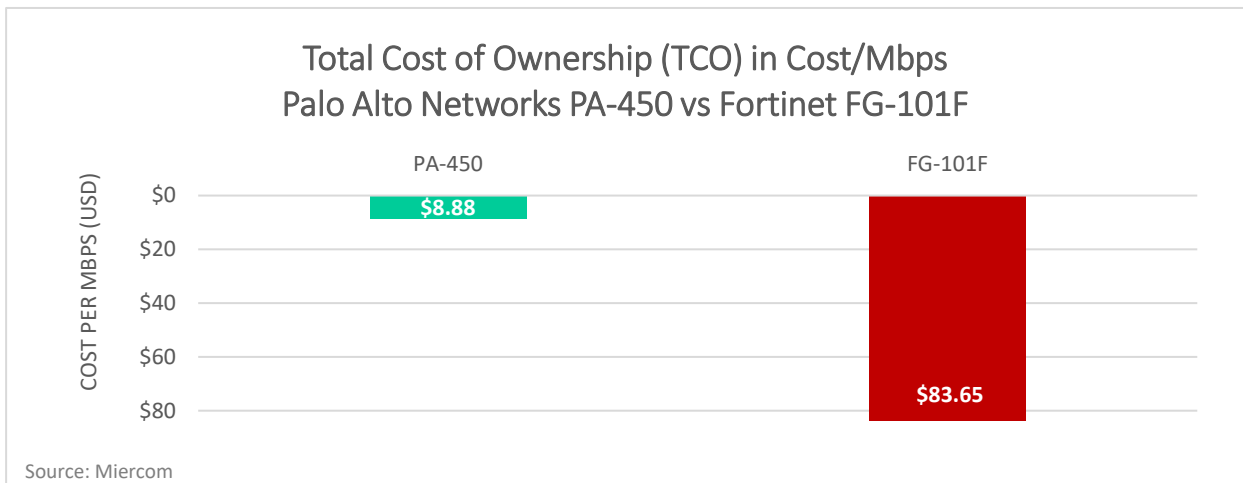
Note: The the total costs of acquisition are based on prices as of July 1st 2021



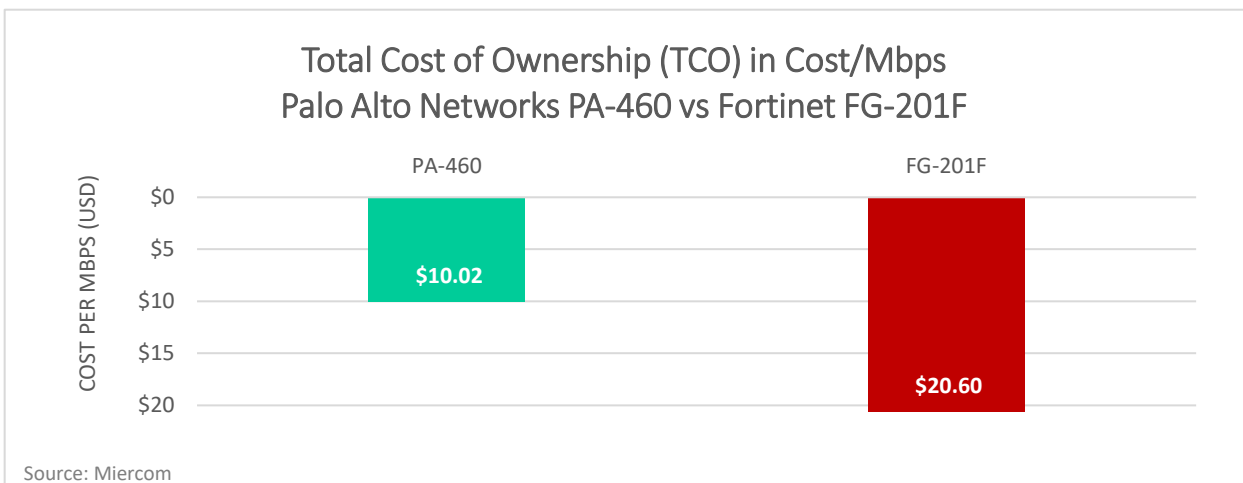
Palo Alto Networks PA-410 offers an 86 percent cost savings per Mbps when compared to the Fortinet FG-61F appliance, which has a substantially higher cost of about \$36 per Mbps. Fortinet costs more in hardware, subscriptions and support, while providing about a fifth of the performance. PA-410 had an average throughput of 390 Mbps, compared to the 74 Mbps seen by FG-61F. When comparing total costs, Palo Alto Networks PA-410 saves customers 23 percent with a total cost of \$2,035; Fortinet FG-61F costs \$2,640.



Palo Alto Networks PA-440 offers an 81 percent cost savings per Mbps when compared to the Fortinet FG-81F appliance, which has a substantially higher cost of about \$21 per Mbps. Fortinet costs higher in hardware, subscriptions and support, while providing about a third of the performance. PA-440 had an average throughput of 731 Mbps, compared to the 218 Mbps seen by FG-81F. When comparing total costs, Palo Alto Networks PA-440 saves customers 35 percent with a total cost of \$2,990; Fortinet FG-81F costs \$4,573.



Palo Alto Networks PA-450 offers an 89 percent cost savings per Mbps when compared to the Fortinet FG-101F appliance, which has a substantially higher cost of about \$84 per Mbps. Fortinet costs more in hardware, subscriptions and support, while PA-450 provides over 6.5 times the performance. PA-450 had an average throughput of 926 Mbps, compared to the 141Mbps seen by FG-101F. When comparing total costs, Palo Alto Networks PA-450 saves customers 30 percent with a total cost of \$8,230; Fortinet FG-101F costs \$11,771.



Palo Alto Networks PA-460 offers a 51 percent cost savings per Mbps when compared to the Fortinet FG-201F appliance, which has a substantially higher cost of about \$21 per Mbps. Fortinet costs more in hardware, subscriptions and support, while PA-460 provides almost twice the performance. PA-460 had an average throughput of 1,240 Mbps, compared to the 702 Mbps seen by FG-201F. When comparing total costs, Palo Alto Networks PA-460 saves customers 14 percent with a total cost of \$12,420; Fortinet FG-201F costs \$14,455.

About Miercom Performance Verified

This report was sponsored by Palo Alto Networks. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied; Miercom accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: <https://miercom.com/tou>.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Security Services

Palo Alto Networks offers the following security services.

- **Threat Prevention:** Goes beyond traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance
 - **Advanced URL Filtering:** Provides best in class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protections
 - **Wildfire:** Ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading cloud-based analysis and crowd-sourced intelligence from over 42,000 customers
 - **DNS Security:** Harnesses the power of machine learning to detect and prevent threats over DNS in real-time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
 - **IoT Security:** Provides the industry's most comprehensive IoT Security solution delivering ML-powered visibility, prevention, and enforcement in a single platform
 - **Enterprise DLP:** The industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users
 - **SaaS Security:** Delivers integrated SaaS Security, that lets you see and secure new SaaS applications, protect data and prevent zero day threats at the lowest TCO.
-

Test Results

Fortinet devices showed very low SIP throughput. To work around the problem, the steps to disable SIP ALG listed in the knowledge base here (<https://kb.fortinet.com/kb/documentLink.do?externalID=FD36405>) were attempted, but it did not resolve the issue. It is our conclusion that SIP traffic is not being reliably processed by these Fortigate devices".

Test	PA-410			FG-61F		
	Services off	Services on	Degradation (%)	Services off	Services on	Degradation (%)
5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)						
	424	287	32.3%	1,152	129	88.8%
5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload						
64K Bandwidth	1,054	843	20.0%	205	74	63.9%
64K CPS	1,752	2,907	-65.9%	3,649	1,350	63.0%
21K Bandwidth	655	620	5.34%	282	162	42.6%
21K CPS	3,159	3,004	4.91%	3,357	1,465	56.4%
4.5K Bandwidth	227	147	35.2%	727	43	94.1%
4.5K CPS	5,172	2,555	50.6%	13,690	1,078	92.1%
5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20						
SIP (Telephony)	516	484	6.20%	4	2	50.0%
MySQL (Database)	237	219	7.59%	298	105	64.8%
FIX (Financial)	147	127	13.6%	N/A	N/A	N/A
5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)						
Max Concurrent TCP Sessions	63,001	42,523	32.5%	526,139	18,165	96.5%
Max TCP CPS	5,231	4,465	14.6%	30,280	1,972	93.5%

Test	PA-440			FG-81F		
	Services off	Services on	Degradation (%)	Services off	Services on	Degradation (%)
5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)						
	811	737	9.12%	319	178	44.2%
5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload						
64K Bandwidth	1,811	1,811	0%	2,143	638	70.2%
64K CPS	2,998	2,998	0%	3,979	1,000	74.9%
21K Bandwidth	1,015	903	11.0%	2,000	427	78.7%
21K CPS	5,693	5,493	3.51%	19,990	1,946	90.3%
4.5K Bandwidth	439	414	5.69%	2,157	115	94.7%
4.5K CPS	6,286	6,286	0%	42,760	1,921	95.5%
5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20						
SIP (Telephony)	731	677	7.39%	3	3	0%
MySQL (Database)	200	192	4.00%	2,258	192	91.5%
FIX (Financial)	440	440	0%	N/A	N/A	N/A
5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)						
Max Concurrent TCP Sessions	158,543	155,528	1.90%	1,331,217	545,478	59.0%
Max TCP CPS	9,496	8,594	9.50%	40,330	2,651	93.4%

Test	PA-450			FG-101F		
	Services off	Services on	Degradation (%)	Services off	Services on	Degradation (%)
5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)						
	1,080	933	13.6%	1,268	248	80.4%
5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload						
64K Bandwidth	2,149	2,134	0.698%	2,150	344	84.0%
64K CPS	4,010	3,980	0.748%	3,755	724	80.7%
21K Bandwidth	1,239	1,237	0.161%	391	52	86.7%
21K CPS	5,999	5,997	0.0333%	3,984	1,131	71.6%
4.5K Bandwidth	499	443	11.2%	1,938	75	96.1%
4.5K CPS	8,845	7,602	14.1%	36,110	1,382	96.2%
5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20						
SIP (Telephony)	986	972	1.42%	5	17	-240%
MySQL (Database)	245	241	1.63%	1359	249	81.7%
FIX (Financial)	594	525	11.6%	N/A	N/A	N/A
5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)						
Max Concurrent TCP Sessions	306,175	134,393	56.1%	1,226,825	36,315	97.0%
Max TCP CPS	13,380	11,920	10.9%	47,720	3,211	93.3%

Test	PA-460			FG-201F		
	Services off	Services on	Degradation (%)	Services off	Services on	Degradation (%)
5.1 Raw TCP Throughput with 1460-Byte Payload (Mbps)						
	1,525	1,440	5.57%	2,038	371	81.8%
5.2 Maximum HTTP 1.1 Connections/sec (CPS) and Bandwidth (Mbps) with 64/21/4.5K Payload						
64K Bandwidth	2,165	2,144	0.970%	2,155	2,089	3.06%
64K CPS	7,000	6,943	0.814%	4,982	4,944	0.763%
21K Bandwidth	2,156	1,960	9.09%	2,189	1,518	30.7%
21K CPS	10,480	9,493	9.42%	10,670	7,388	30.8%
4.5K Bandwidth	760	650	14.5%	2,166	432	80.1%
4.5K CPS	14,590	12,370	15.2%	40,130	7,969	80.1%
5.3 Single Application Performance (Mbps) before "Application Transaction Failures" exceed 20						
SIP (Telephony)	1,400	1,440	0%	5	5.4	-8.00%
MySQL (Database)	287	287	0%	842	497	41.0%
FIX (Financial)	799	748	6.38%	N/A	N/A	N/A
5.4 Maximum TCP Capacity Concurrent TCP Sessions and Connections/sec (CPS)						
Max Concurrent TCP Sessions	459,278	440,288	4.13%	3,222,535	742,696	77.0%
Max TCP CPS	19,420	17,360	10.6%	120,100	16,020	86.7%